FICHE 6

CyB3R $3cuR1Ty

La cyber sécurité vous inquiète en tant qu'adulte et... elle effleure certainement l'esprit de vos élèves/jeunes qui, paradoxalement, se sentent assez experts en la matière. Même s'iels ont régulièrement tendance à se sentir suffisamment outillé·es par rapport à cette thématique, vous vous apercevrez assez vite qu'il n'en est rien. Il reste primordial de l'aborder (d'ailleurs la fiche 9 - pigeon est un beau complément).

Les POV rejoignent tous une problématique de base: le mot de passe. Leur mauvais usage a pour conséquence : le piratage, qui peut entraîner l'usurpation d'identité, les arnaques et le cyber-harcèlement... Voyons cela de plus près.

1234 OU PASSWORD... OU LA NÉCESSITÉ D'UN MOT DE PASSE FORT!

Peut-être pourriez-vous commencer par demander à vos élèves (et à vous-mêmes !) : quels sont les pires mots de passe ? Sachez que le trio de tête est composé par les suites logiques (chiffres comme 1234 ou lettres du clavier comme azerty), des mots usuels comme «password», «motdepasse», «coucou» et enfin, n'importe quel élément facile à trouver sur vous, via les réseaux sociaux, par exemple (adresse, date de naissance, 2ème prénom, surnom, passion, nom d'un animal de compagnie...). Dans tous ces cas, il faut moins d'une seconde à un hacker pour le forcer.

Cette fiche renvoie à cet épisode du podcast

Toutes les ressources liées à la thématique sont disponibles dans ce tableau !

COMMENT FAIRE?

Après cette révélation qui suscitera peut-être la perplexité ou l'effroi dans les yeux de vos élèves/jeunes, il semble important de leur proposer des conseils pour créer un mot de passe fort.

- comporter idéalement 13 caractères de 4 types différents (chiffres, lettres, signes de ponctuation et/ou caractères spéciaux
- La technique du Leet Speak permet la mémorisation plus simple d'un mot de passe. Elle consiste à remplacer certaines lettres par des caractères spéciaux qui leur ressemblent. Par exemple: @ pour a, 3 pour E, 0 pour O,1 pour le i

- être malgré tout facile à retenir (un slogan qui fonctionne bien: «facile à retenir pour toi, difficile à trouver pour les autres»)
- ne pas avoir de «sens»: associer par exemple 3 mots qui ont du sens pour nous mais qui n'ont pas de lien entre eux est utile pour complexifier la tâche du hacker. Par exemple: chien, barque, montagne (devenant avec le Leet Speak Ch13nB@rqu3M0nt@gn3)
- être unique pour chaque compte
- Cela se corse ici... Une méthode à proposer est de garder la même association de mots mais d'y ajouter une abréviation du compte auquel il est destiné. Par exemple:

Pour Instagram = Ch13nB@rqu3M0nt@gn3-IN
Pour Snapchat = Ch13nB@rqu3M0nt@gn3-SN
Pour Discord = Ch13nB@rqu3M0nt@gn3-DI

- ne le révéler à personne. C'est ici qu'une discussion sur la confiance peut s'intégrer...
- ne pas enregistrer son mot de passe dans un ordinateur partagé
- changer de mot de passe régulièrement

En plus de ces règles de base pour sa création, d'autres conseils sont les bienvenus pour l'usage quotidien (à aborder avec des élèves plus âgés ou déjà bien au fait des notions de cyber-sécurité) :

- utiliser un gestionnaire de mot de passe : c'est un service semblable à un coffre-fort pour tous vos mots de passe, vous l'ouvrez avec...un mot de passe! Mais cela n'en fait qu'un à retenir, et il ouvre l'accès à tous les autres.
- activer, quand c'est possible, la double authentification - ou authentification à 2 facteurs. il s'agit de s'identifier de deux manières plutôt que d'une, sachant que, globalement, nos possibilités sont les suivantes: un mot de passe, un code envoyé par mail ou message, une empreinte digitale, une reconnaissance faciale ou une application comme itsme.
- Pour un exercice d'esprit critique, et au regard de tout ce que vous aurez dit précédemment, analysez ensemble le travail effectué par un générateur de mot de passe en ligne (celui du Cnil renseigné dans les ressources, par exemple)

Accorder tant d'importance à ses mots de passe, pour quoi faire ?

Tout simplement, pour se prémunir d'une série de problèmes liés au piratage. On parle aussi de se faire hacker, c'est-à-dire qu'un individu malveillant prend le contrôle, par exemple, d'un compte sur un réseau social dans le but de le détourner (dérober des données personnelles, professionnelles, bancaires, usurper l'identité ...). C'est évidemment tout à fait punissable par la loi.

Mais ces hackers ne sont pas tous des cyber-criminels, organisés et équipés de programmes informatiques perfectionnés pour vous pirater... Dans la réalité de vos élèves/jeunes, pirater le compte d'une autre personne peut leur apparaître comme une «blague». C'est ce qu'on entend dans le POV par le terme «pranker» qui signifie faire un canular, piéger une personne.

Identifions à présent les 3 piratages les plus fréquents:

Le phishing

C'est un terme utilisé pour parler d'arnaques dans lesquelles de faux emails ou messages sont envoyés, par exemple avec un lien vers un site web ou une pièce jointe à ouvrir. Un virus qui peut entraîner la divulgation de vos données personnelles, dont vos données bancaires, peut s'installer. Un site Internet comme www.safeonweb.be vous explique clairement les procédures à suivre si vous êtes victime de phishing.

Même si c'est peut-être la première conséquence du piratage à laquelle penseront vos élèves, il y a de fortes chances qu'ils soient moins concernés par ce type de piratage que par les deux suivants.

- L'usurpation d'identité

Il s'agit bien du processus dans lequel quelqu'un prend possession d'un compte qui n'est pas le sien, sans autorisation du propriétaire légitime, et se fait passer pour lui. Qu'il s'agisse d'un faux compte de star (pour profiter de l'image de la personne et faire de la publicité mensongère) ou pour en tirer des profits malhonnêtes, cette pratique est évidemment interdite par la loi. En effet, en plus d'être frauduleuse, elle n'est pas respectueuse du droit à l'image. Un conseil important pour les jeunes est de le signaler avant tout à la plateforme sur laquelle se présente le problème. Les réseaux sociaux rendent cet accès de plus en plus facile via leurs paramètres. Et si cette étape ne suffit pas, il est possible de porter plainte auprès de la police.

- Le cyber-harcèlement.

C'est ce risque qui semble le plus proche de la réalité des adolescent.e.s. Vous qui travaillez avec des jeunes, vous êtes certainement bien au clair avec les situations suivantes: la création d'un compte spécifique pour nuire à une personne (ou sa réputation), le vol de données personnelles (des photos ou des informations privées) ou encore la prise de contrôle d'un compte pour faire tenir des propos problématiques à une victime .

On vous en parle d'ailleurs dans la fiche 7 - le loup, la chèvre et le chou.

E.R. : Ultra Vagues - www.ultravagues.com